(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－175084
（P2002－175084A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ	５Ｊ１０４
Ｇ１０Ｌ　19/00		Ｈ０４Ｍ　1/00	Ｕ	５Ｋ０２７
Ｈ０４Ｌ　9/08		11/00	３０２	５Ｋ１０１

審査請求　未請求　請求項の数９　ＯＬ　（全 28 頁）　最終頁に続く

(21)出願番号　特願2000－372418(P2000－372418)

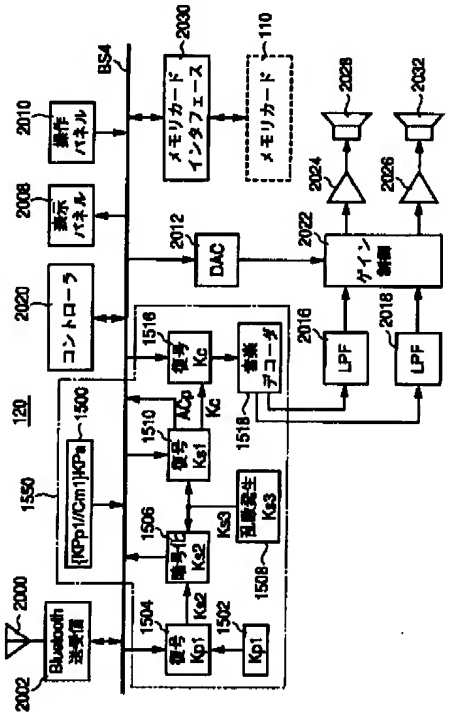
(22)出願日　平成12年12月７日(2000.12.7)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　上村　透
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　再生装置

(57)【要約】
【課題】　暗号化コンテンツデータを通常のコンテンツデータと同じように再生可能な再生装置を提供する。
【解決手段】　ポータブルステレオ１２０は、コンテンツ再生デバイス１５５０を含む。コントローラ２０２０は、アンテナ２０００および送受信部２００２を介して携帯電話機に装着されたメモリカードから暗号化コンテンツデータおよびライセンスを受信して暗号化コンテンツデータおよびライセンスをコンテンツ再生デバイス１５５０に与える。コンテンツ再生デバイス１５５０は、ライセンスによって暗号化コンテンツデータを復号し、かつ、再生してＬＰＦ２０１６，２０１８へ出力する。そして、音楽データは、ＬＰＦ２０１６，２０１８、ゲイン制御部２０２２、増幅器２０２４，２０２６、スピーカ２０２８，２０３２を経て外部へ出力される。



1

【特許請求の範囲】

【請求項１】　暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスとを格納したデータ記録装置が装着された端末通信装置から前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータを前記ライセンスによって再生する再生装置であって、

前記端末通信装置との間でデータの送受信を行なう専用送受信部と、

指示を入力するための操作部と、

前記暗号化コンテンツデータを前記ライセンスによって再生するコンテンツ再生部と、

前記コンテンツ再生部によって再生されたコンテンツデータを外部へ出力するための出力部と、

制御部とを備え、

前記制御部は、前記操作部から入力された暗号化コンテンツデータの再生指示に応じて、前記専用送受信部を介して前記端末通信装置へアクセスし、前記端末通信装置によって前記データ記録装置から読出された暗号化コンテンツデータおよびライセンスを前記専用送受信部を介して受信し、その受信した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生部へ与える、再生装置。

【請求項２】　前記端末通信装置の電源部を充電するための充電部をさらに備える、請求項１に記載の再生装置。

【請求項３】　前記端末通信装置を介して通話するためのハンドフリーな通話部をさらに備える、請求項１に記載の再生装置。

【請求項４】前記通話部は、

ユーザの音声を入力するための入力部と、

通話相手の音声を外部へ出力するための音声出力部と、

前記専用送受信部からの前記通話相手の音声信号を復号し、その復号した音声を前記音声出力部に与え、前記入力部からの音声を所定の方式に符号化し、その符号化した音声信号を前記専用送受信部に与える復号／符号部とを含む、請求項３に記載の再生装置。

【請求項５】　前記データ記録装置を装着するための装着部と、

前記データ記録装置との間でデータの授受を制御するためのインタフェースとをさらに備え、

前記装着部に前記データ記録装置が装着されたとき、

前記制御部は、前記操作部から入力された暗号化コンテンツデータの再生指示に応じて、前記インタフェースを介して前記データ記録装置から暗号化コンテンツデータおよびライセンスを取得し、その取得した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生部へ与える、請求項１から請求項４のいずれか１項に記載の再生装置。

【請求項６】　前記コンテンツ再生部は、前記データ記録装置に対する認証データを保持する認証データ保持部を含み、

前記制御部は、前記認証データを前記専用送受信部を介して前記端末通信装置へ送信し、前記データ記録装置において前記認証データが認証されると、前記専用送受信部を介して前記暗号化コンテンツデータおよび前記ライセンスを受信する、請求項１から請求項４のいずれか１項に記載の再生装置。

【請求項７】　前記コンテンツ再生部は、

第１の共通鍵を発生する共通鍵発生部と、

前記第１の共通鍵による復号処理を行なう復号処理部と、

前記データ記録装置において発生された第２の共通鍵によって前記第１の共通鍵を暗号化する暗号処理部とをさらに含み、

前記制御部は、前記第２の共通鍵によって暗号化された第１の共通鍵を前記専用送受信部を介して前記端末通信装置へ送信し、前記端末通信装置から前記第１の共通鍵によって暗号化されたライセンス鍵を受信して前記コンテンツ再生部に与える、請求項６に記載の再生装置。

【請求項８】　前記コンテンツ再生部は、前記データ記録装置に対する認証データを保持する認証データ保持部を含み、

前記制御部は、前記データ記録装置が前記端末通信装置に装着された場合、前記認証データを、前記専用送受信部を介して前記端末通信装置へ送信し、前記専用送受信部を介して、少なくとも前記ライセンスを受信し、前記データ記録装置が前記装着部に装着された場合、前記インタフェースを介して前記認証データを前記データ記録装置に与え、前記データ記録装置において前記認証データが認証されると、前記インタフェースを介して、前記ライセンスと前記暗号化コンテンツデータとを受信する、請求項５に記載の再生装置。

【請求項９】　前記コンテンツ再生部は、

第１の共通鍵を発生する共通鍵発生部と、

前記第１の共通鍵による復号処理を行なう復号処理部と、

前記データ記録装置において発生された第２の共通鍵によって前記第１の共通鍵を暗号化する暗号処理部とをさらに含み、

前記制御部は、前記データ記録装置が前記端末通信装置に装着された場合、前記第２の共通鍵によって暗号化された第１の共通鍵を前記専用送受信部を介して前記端末通信装置へ送信し、前記端末通信装置から前記第１の共通鍵によって暗号化されたライセンスを受信して前記コンテンツ再生部に与え、前記データ記録装置が前記装着部に装着された場合、前記第２の共通鍵によって暗号化された第１の共通鍵を、前記インタフェース部を介して前記データ記録装置へ与え、前記データ記録装置から前記第１の共通鍵によって暗号化されたライセンスを受信

して前記コンテンツ再生部に与える、請求項８に記載の再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられる再生装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が

講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】

【発明が解決しようとする課題】しかし、携帯電話機以外に、暗号化コンテンツデータを再生する機能を持つ再生装置がないため、通常の音楽データとともに暗号化コンテンツデータを再生できないという問題がある。

【００１５】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、暗号化コンテンツデータを通常のコンテンツデータと同じように再生可能な再生装置を提供することである。

【００１６】

【課題を解決するための手段および発明の効果】この発明による再生装置は、暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスとを格納したデータ記録装置が装着された端末通信装置から暗号

化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータをライセンスによって再生する再生装置であって、端末通信装置との間でデータの送受信を行なう専用送受信部と、指示を入力するための操作部と、暗号化コンテンツデータをライセンスによって再生するコンテンツ再生部と、コンテンツ再生部によって再生されたコンテンツデータを外部へ出力するための出力部と、制御部とを備え、制御部は、操作部から入力された暗号化コンテンツデータの再生指示に応じて、専用送受信部を介して端末通信装置へアクセスし、端末通信装置によってデータ記録装置から読出された暗号化コンテンツデータおよびライセンスを専用送受信部を介して受信し、その受信した暗号化コンテンツデータおよびライセンスをコンテンツ再生部へ与える。

【００１７】この発明による再生装置においては、端末通信装置との間でデータのやり取りを通信によって行ない、端末通信装置に装着されたデータ記録装置から暗号化コンテンツデータおよびライセンスを受信し、暗号化コンテンツデータを再生する。

【００１８】したがって、この発明によれば、暗号化コンテンツデータを、直接、取得することができない再生装置においても、暗号化コンテンツデータを再生することができる。

【００１９】好ましくは、再生装置は、端末通信装置の電源部を充電するための充電部をさらに備える。

【００２０】再生装置は、端末通信装置が装着されると、端末通信装置の電源部を充電する。

【００２１】したがって、この発明によれば、再生装置は暗号化コンテンツデータをデータ記録装置から受信するのに必要な端末通信装置と一体化できる。

【００２２】好ましくは、再生装置は、端末通信装置を介して通話するためのハンドフリーな通話部をさらに備える。

【００２３】入力されたユーザの音声は通話部によって所定の符号化を施され、専用送受信部を介して端末通信装置へ送信され、端末通信装置からの音声信号は通話部によって復号され再生装置のユーザに与えられる。

【００２４】したがって、この発明によれば、ユーザは、暗号化コンテンツデータを再生できるとともに、通話部を介して他の人とも通話をできる。

【００２５】好ましくは、再生装置の通話部は、ユーザの音声を入力するための入力部と、通話相手の音声を外部へ出力するための音声出力部と、専用送受信部からの通話相手の音声信号を復号し、その復号した音声を音声出力部に与え、入力部からの音声を所定の方式に符号化し、その符号化した音声信号を専用送受信部に与える復号／符号部とを含む。

【００２６】通話部は、音声を音声信号へ符号化し、音声信号を音声に復号する。したがって、この発明によれば、ユーザは、暗号化コンテンツデータを再生できるとともに、通話部を介して他の人とも通話をできる。

【００２７】好ましくは、再生装置は、データ記録装置を装着するための装着部と、データ記録装置との間でデータの授受を制御するためのインタフェースとをさらに備え、装着部に前記データ記録装置が装着されたとき、制御部は、操作部から入力された暗号化コンテンツデータの再生指示に応じて、インタフェースを介してデータ記録装置から暗号化コンテンツデータおよびライセンスを取得し、その取得した暗号化コンテンツデータおよびライセンスをコンテンツ再生部へ与える。

【００２８】再生装置は、装着されたデータ記録装置から暗号化コンテンツデータとライセンスとを取得し、その取得した暗号化コンテンツデータをライセンスによって再生する。

【００２９】したがって、この発明によれば、他の装置に装着することによって暗号化コンテンツデータおよびライセンスを取得したデータ記録装置を装着して暗号化コンテンツデータを再生できる。

【００３０】好ましくは、再生装置のコンテンツ再生部は、データ記録装置に対する認証データを保持する認証データ保持部を含み、制御部は、認証データを専用送受信部を介して端末通信装置へ送信し、データ記録装置において認証データが認証されると、専用送受信部を介して暗号化コンテンツデータおよびライセンスを受信する。

【００３１】再生装置は、コンテンツ再生部が正規の機器であることが認証されると、暗号化コンテンツデータとライセンスとを受信する。そして、コンテンツ再生部は、暗号化コンテンツデータをライセンスによって再生する。

【００３２】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【００３３】好ましくは、再生装置のコンテンツ再生部は、第１の共通鍵を発生する共通鍵発生部と、第１の共通鍵による復号処理を行なう復号処理部と、データ記録装置において発生された第２の共通鍵によって第１の共通鍵を暗号化する暗号処理部とをさらに含み、制御部は、第２の共通鍵によって暗号化された第１の共通鍵を専用送受信部を介して端末通信装置へ送信し、端末通信装置から第１の共通鍵によって暗号化されたライセンス鍵を受信してコンテンツ再生部に与える。

【００３４】コンテンツ再生部とデータ記録装置との間で、相互に発生させた共通鍵をやり取りすることによって安全な暗号化通信路を確保して、コンテンツ再生部は自己が発生した共通鍵によって暗号化されたライセンス鍵を受信する。

【００３５】したがって、この発明によれば、より安全に暗号化コンテンツデータを再生できる。

【００３６】好ましくは、再生装置のコンテンツ再生部は、データ記録装置に対する認証データを保持する認証

データ保持部を含み、制御部は、データ記録装置が端末通信装置に装着された場合、認証データを、専用送受信部を介して端末通信装置へ送信し、専用送受信部を介して、少なくともライセンスを受信し、データ記録装置が装着部に装着された場合、インタフェースを介して認証データをデータ記録装置に与え、データ記録装置において認証データが認証されると、インタフェースを介して、ライセンスと暗号化コンテンツデータとを受信する。

【００３７】再生装置のコンテンツ再生部は、データ記録装置に対する認証データが認証されると、データ記録装置からライセンスと暗号化コンテンツデータとを受信し、ライセンスによって暗号化コンテンツデータを再生する。

【００３８】したがって、この発明によれば、正規のコンテンツ再生部を有する再生装置だけがデータ記録装置から暗号化コンテンツデータとライセンスとを受信し、暗号化コンテンツデータを再生できる。

【００３９】好ましくは、再生装置のコンテンツ再生部は、第１の共通鍵を発生する共通鍵発生部と、第１の共通鍵による復号処理を行なう復号処理部と、データ記録装置において発生された第２の共通鍵によって第１の共通鍵を暗号化する暗号処理部とをさらに含み、制御部は、データ記録装置が端末通信装置に装着された場合、第２の共通鍵によって暗号化された第１の共通鍵を専用送受信部を介して端末通信装置へ送信し、端末通信装置から第１の共通鍵によって暗号化されたライセンスを受信してコンテンツ再生部に与え、データ記録装置が装着部に装着された場合、第２の共通鍵によって暗号化された第１の共通鍵を、インタフェース部を介してデータ記録装置へ与え、データ記録装置から第１の共通鍵によって暗号化されたライセンスを受信してコンテンツ再生部に与える。

【００４０】再生装置は、データ記録装置との間で共通鍵による相互認証を行ない、相互に認証された場合にデータ記録装置からライセンスを受信する。

【００４１】したがって、この発明によれば、暗号化コンテンツデータを再生するライセンスをデータ記録装置から再生装置へより安全に送信できる。

【００４２】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００４３】図１は、本発明による再生装置（カーステレオまたはコンポーネントステレオ）が再生の対象とする暗号化コンテンツデータを通信機能を有する通信装置に配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００４４】なお、以下では携帯電話網を介して音楽データを各携帯電話機に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等を配信する場合においても適用することが可能なものである。また、インターネット網や直接ダイアルアップ接続による公衆電話網への適用も可能である。

【００４５】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話機からの配信要求（配信リクエスト）を配信サーバ１０に中継する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００４６】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００４７】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００４８】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００４９】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００５０】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００５１】暗号化コンテンツデータおよびライセンス

を受信したメモリカード１１０は、カーステレオまたはコンポーネントステレオ等のポータブルステレオ１２０からの暗号化コンテンツデータの再生許諾要求に応じて、ポータブルステレオ１２０に内蔵されたコンテンツ再生デバイス（図示せず）の正当性を認証データに基づいて確認し、ライセンスを、携帯電話機１００を介して通信によってポータブルステレオ１２０へ送信する。次いで、ポータブルステレオ１２０からの暗号化コンテンツデータの送信要求に対して、暗号化コンテンツデータを、携帯電話機１００を介して通信によってポータブルステレオ１２０へ送信する。そして、ポータブルステレオ１２０は、暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスによって暗号化コンテンツデータを再生する。

【００５２】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機またはポータブルステレオのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第２には、通信においてライセンスを安全に配信するための方式であり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツ保護を実現する構成である。

【００５３】なお、以下の説明においては、配信サーバ１０から、各携帯電話機に暗号化コンテンツデータおよびライセンスを伝送する処理を「配信」と称することとする。

【００５４】本発明の実施の形態においては、特に、配信、および再生において、これらのライセンスの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られたような不正な記録装置および再生装置（コンテンツを再生できるコンテンツ再生デバイスを備えた再生装置、必要に応じてポータブルステレオまたは携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００５５】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００５６】まず、配信サーバ１０より配信されるデータについて説明する。コンテンツデータＤｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話ユーザに配布される。

【００５７】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００５８】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する情報あるいはサーバのアクセスに関する情報等を含む平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、配信サーバ１０からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ１０と携帯電話機１００との間でやり取りされる。さらに、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤおよび著作権者の許可範囲内において、利用者側からの指示であり、ライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する条件を示すアクセス制限ＡＣｍおよびデータ再生端末における再生条件を示す制御情報である再生制限ＡＣｐが存在する。具体的には、アクセス制限ＡＣｍはメモリカードからのライセンスまたはライセンス鍵を外部に出力に対するにあたっての制限情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生の特殊再生や期間を制限する制限情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００５９】以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵ＫｃとライセンスＩＤとアクセス制限ＡＣｍと再生制限ＡＣｐとを併せて、ライセンスと総称することとする。

【００６０】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機またはポータブルステレオのクラスごとに、コンテンツデータの配信、および再生を禁止することができるように証明書失効リストＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって証明書失効リスト内のデータを表わすこともある。

【００６１】証明書失効リスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機、メモリカード、およびコンテンツ再生デバイスのクラス証明書をリストアップした証明書失効リストデータＣＲＬが含まれる。

【００６２】証明書失効リストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカードにも記録保持される。このような証明書失効リストは、随時、更新していく必要があるが、データの変更については、基本的にはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から証明書失効リストの更新日時を判断し、更新されていないとき、新しい証明書失効リストを携帯電話機に配信する。また、証明書失効リストの変更については、変更点のみを反映した差分

データである差分ＣＲＬを配信サーバ１０側より発生して、これに応じてメモリカードの証明書失効リストＣＲＬが書替えられる構成とするも可能である。また、証明書失効リストの更新日時については、メモリカード側より出力し、これを配信サーバ１０側で確認することによって更新日時の管理を実行する。差分ＣＲＬには更新日時ＣＲＬｄａｔｅも含まれる。

【００６３】このように、証明書失効リストＣＲＬを、配信サーバのみならずメモリカードにおいても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードまたはコンテンツ再生デバイスの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードまたはコンテンツ再生デバイスへのライセンス鍵の供給を禁止する。このため、携帯電話機またはコンテンツ再生デバイスではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。クラスについては、後ほど詳細に説明する。

【００６４】このように、メモリカードの証明書失効リストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカードにおける証明書失効リストＣＲＬの管理は、上位レベルとは独立にメモリカードでタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから証明書失効リストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００６５】図３は、図１に示すデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

【００６６】メモリカード、およびコンテンツ再生デバイスには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは携帯電話機に固有の秘密復号鍵Ｋｐｙおよびメモリカードに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、クラス鍵を共有する単位をクラスと称する。

【００６７】また、コンテンツ再生デバイスのクラス証明書としてＣｐｙが設けられ、メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生デバイス、およびメモリカードのクラスごと、すなわちクラス鍵単位に異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、証明書失効リストにリストアップされてライセンス発行の禁止対象となる。

【００６８】これらのコンテンツ再生デバイス、およびメモリカードに固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式または認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生デバイス、およびメモリカードにそれぞれ記録される。ＫＰａは配信システム全体で共通の公開認証鍵であり、認証データを復号することで、その正当性を確認することができる。公開認証鍵ＫＰａは、配信サーバ１０およびメモリカード１１０内に保持される。

【００６９】また、メモリカード１１０のデータ処理を管理するための鍵として、メモリカードという媒体ごとに個別に設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍｃｘが存在する。

【００７０】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、メモリカード１１０、コンテンツ再生デバイス（携帯電話機１００、ポータブルステレオ１２０）において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００７１】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生デバイスもしくはメモリカードもしくはコンテンツ再生デバイス間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００７２】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、メモリカード、およびコンテンツ再生デバイスによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００７３】図４は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、暗号化コンテンツデータのコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、パーソナルコンピュータの各ユーザごとにライセンス鍵等へのアクセス開始に従った課金情報を保持するための課金データベース３０２と、証明書失効リストＣＲＬを管理するＣ

ＲＬデータベース３０６と、情報データベース３０４に保持されたライセンスによって再生されるコンテンツデータのメニューを保持するメニューデータベース３０７と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等を含む、配信のログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００７４】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、携帯電話機１００から送られてきた認証のためのメモリカード１１０の認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｘを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００７５】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制限ＡＣｍを、復号処理部３２０によって得られたメモリカードに固有の公開暗号鍵ＫＰｍｗによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００７６】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７７】図５は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００７８】携帯電話機１００は、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０１と、アンテナ１１０１からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０１に与えるための送受信部１１０２と、ポータブルステレオ１２０からの信号を受信するためのアンテナ１１０３と、アンテナ１１０３からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機１００からのデータを変調してアンテナ１１０３に与えるための送受信部１１０４と、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００７９】携帯電話機１００は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００とを含む。

【００８０】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生デバイス）の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ２およびクラス証明書Ｃｐ２を公開復号鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ２／／Ｃｐ２｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、携帯電話機（データ端末装置）１００のクラスｙは、ｙ＝２であるとする。

【００８１】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生デバイス）固有の復号鍵であるＫｐ２を保持するＫｐ保持部１５０２と、バスＢＳ２から受けたデータをＫｐ２によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００８２】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制限ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ３に出力する暗号処理部１５０６とを含む。

【００８３】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１５１０と、バスＢＳ２より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータＤｃを再

生するための音楽デコーダ１５１８と、混合器１１１８の出力を外部出力装置（図示省略）へ出力するための端子１１２０とを含む。

【００８４】携帯電話機１００は、さらに、ユーザの音声を入力するためのマイク１１１４と、マイク１１１４からの音声を符号化してバスＢＳ２に与え、またはバスＢＳ２上の音声信号を復号してスピーカ１１１６に与える音声処理部１１１２と、音声処理部１１１２部からの音声信号を外部へ出力するためのスピーカ１１１６と、音声処理部１１１２からの音声信号または音楽デコーダ１５１８からの音楽信号を混合して端子１１２０へ出力するための混合器１１１８とを含む。

【００８５】なお、図５においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。また、図５においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【００８６】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８７】図６は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有のクラス鍵である公開暗号鍵および秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、これらはクラスｗは、ｗ＝７で表わされるものとする。また、メモリカードごとに個別に設けられる個別なメモリカードを識別する識別子ｘは、ｘ＝８で表されるものとする。

【００８８】したがって、メモリカード１１０は、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵であるＫｍｃ８を保持するＫｍｃ保持部１４０２と、メモリカードの種類ごとに設定される固有の秘密復号鍵Ｋｍ７を保持するＫｍ保持部１４２１と、Ｋｍｃ８によって復号可能な公開暗号鍵ＫＰｍｃ８を保持するＫＰｍｃ保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａとして保持する。

【００８９】このように、メモリカードという記録装置に固有の暗号鍵および復号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００９０】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を、端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、メモリカードのクラスごとに固有の秘密復号鍵Ｋｍ７をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から認証鍵ＫＰａを受けて、バスＢＳ４に与えられるデータからＫＰａによる復号処理を実行して復号結果を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号処理部１４０６とを含む。

【００９１】メモリカード１１０は、さらに、再生セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるコンテンツ再生デバイスのクラス鍵である公開暗号鍵ＫＰｐｙもしくは他のメモリカードのクラス鍵である公開暗号鍵ＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制限ＡＣｐを、復号処理部１４１２で復号された移動セッションにおいて他のメモリカードに固有な公開暗号鍵ＫＰｍｃｘ（ｘ≠８）で暗号化する暗号処理部１４１７とを含む。

【００９２】メモリカード１１０は、さらに、バスＢＳ４上のデータを公開暗号鍵ＫＰｍｃ８と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍｃ８によって復号するための復号処理部１４０４と、逐次更新される証明書失効リストデータＣＲＬと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、証明書失効リストＣＲＬを記録したＣＲＬ領域１４１５Ａと、ライセンスを記録したライセンス領域１４１５Ｂと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆを記録したデータ領域１４１５Ｃとから成る。

【００９３】また、ＣＲＬ領域１４１５Ａおよびライセ

ンス領域１４１５Ｂは、外部から直接アクセス不可能なセキュアなメモリ空間に設けられる。データ領域１４１５Ｃは外部からアクセス可能な通常のメモリ空間に設けられる。

【００９４】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【００９５】図７は、ポータブルステレオ１２０の構成を示す概略ブロック図である。ポータブルステレオ１２０は、ポータブルステレオを構成する各部とのデータの授受を行なうバスＢＳ４と、携帯電話機１００からの信号を受信するアンテナ２０００と、アンテナ２０００によって受信された信号をベースバンド信号に変換し、あるいはポータブルステレオからのデータを変調してアンテナ２０００に与えるための送受信部２００２と、メモリカード１１０に配信された暗号化コンテンツデータとライセンスとを携帯電話機１００による通信によって受信し、その受信したライセンスによって暗号化コンテンツデータを再生するコンテンツ再生デバイス１５５０とを含む。なお、コンテンツ再生デバイス１５５０は、図５に示すコンテンツ再生デバイスと同じ構成であるが、ポータブルステレオ１２０のコンテンツ再生デバイスにおいては、ポータブルステレオに固有なクラスｙをｙ＝１とする。したがって、認証データを｛ＫＰｐ２／／Ｃｐ２｝ＫＰａから｛ＫＰｐ１／／Ｃｐ１｝ＫＰａに代え、Ｋｐ保持部１５０２に保持する秘密復号鍵をＫｐ保持部１５０２に代えている。その以外の部分については、図５に示したコンテンツ再生デバイスと同じである。

【００９６】ポータブルステレオ１２０は、さらに、バスＢＳ４を介してポータブルステレオ１２０の動作を制御するためのコントローラ２０２０と、外部からの指示をポータブルステレオ１２０に与えるための操作パネル２０１０と、コントローラ２０２０等から出力される情報をポータブルステレオのユーザに視覚情報として与えるための表示パネル２００８とを含む。

【００９７】ポータブルステレオ１２０は、さらに、コンテンツ再生デバイス１５５０の音楽デコーダ１５１８からの音楽信号をＬチャンネルのスピーカ用の音楽信号とＲチャンネルのスピーカ用の音楽信号とに分離し、それぞれの音楽信号のノイズを除去するＬＰＦ２０１６，２０１８と、コントローラ２０２０からの指示信号をバスＢＳ４から受けてデジタル信号からアナログ信号に変換するＤＡ変換器２０１２と、ＤＡ変換器２０１２からのアナログ信号によって増幅率を制御するゲイン制御部２０２２とを含む。

【００９８】ポータブルステレオ１２０は、さらに、ゲイン制御部２０２２により制御された増幅率によってＬＰＦ２０１６，２０１８からのアナログ信号を、それぞれ、増幅する増幅器２０２４，２０２６と、増幅器２０２４からの信号を外部へ出力するスピーカ２０２８と、増幅器２０２６からの信号を外部へ出力するスピーカ２０３２とを含む。

【００９９】以降では、簡単化のためアクセス制限ＡＣｍは再生回数の制限を行なう制御情報である再生回数のみを、再生制限ＡＣｐは再生可能な期限を規定する制御情報である再生期限のみを制限するものとする。

【０１００】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１０１】［配信］図１に示すデータ配信システムにおいて、配信サーバ１０から携帯電話機１００へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【０１０２】図８～図１１は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機１００への配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１０３】図８における処理以前に、携帯電話機１００のユーザは、配信サーバ１０に携帯電話網を介して接続し、配信サーバ１０のメニューデータベース３０７から提供されるメニューに従って配信（購入）を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０１０４】図８を参照して、携帯電話機１００のユーザから操作パネル１１０８を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、操作パネル１１０８を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンスを購入するために、暗号化コンテンツデータのアクセス制限ＡＣｍ、および再生制限ＡＣｐを設定するための購入条件ＡＣが入力される。

【０１０５】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの出力指示を受取る。そして、コントローラ１４２０は、バスＢＳ３を介して認証データ保持部１４００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをバスＢＳ３、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０６）。

【０１０６】携帯電話機１００のコントローラ１１０６は、メモリカード１１０からの認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａに加えて、コンテンツＩＤ、ライセン

ス購入条件ＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０１０７】配信サーバ１０では、携帯電話機１００から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ、およびライセンス購入条件ＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてメモリカード１１０に出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０１０８】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍ７と証明書Ｃｍ７とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を受理しないで処理を終了する（ステップＳ１９８）。

【０１０９】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍ７が証明書失効リストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が証明書失効リストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０１１０】一方、メモリカード１１０のクラス証明書が証明書失効リストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０１１１】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが証明書失効リストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍ７によって、暗号処理部３１８によって暗号化される（ステップＳ１２２）。

【０１１２】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１１３】図９を参照して、携帯電話機１００が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７を受信すると

（ステップＳ１２６）、コントローラ１１０６は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７をメモリカード１１０に入力する（ステップＳ１２８）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを、復号処理部１４２２が、保持部１４２１に保持されるメモリカード１１０に固有の秘密復号鍵Ｋｍ７により復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０１１４】コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０１１５】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている証明書失効リストの更新日時ＣＲＬｄａｔｅを抽出して切換スイッチ５２４６に出力する（ステップＳ１３４）。

【０１１６】暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍｃ８および更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０１１７】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース１４２４および端子１４２６を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ１０に送信される（ステップＳ１３８）。

【０１１８】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍｃ８およびメモリカード１１０における証明書執行リストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ１４２）。

【０１１９】配信制御部３１５は、ステップＳ１１０で取得したコンテンツＩＤおよびライセンス購入条件ＡＣに従って、アクセス制限ＡＣｍおよび再生制限ＡＣｐを生成する（ステップＳ１４４）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１４６）。

【０１２０】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制限ＡＣｐ、およびアクセス制限ＡＣｍを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍｃ８によってライセンスを暗号化して暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を生成する（ステップＳ１４８）。

【０１２１】図１０を参照して、配信サーバ１０において、メモリカード１１０から送信された証明書失効リストの更新日時ＣＲＬｄａｔｅが、ＣＲＬデータベース３０６に保持される配信サーバ１０における失効証明書リストＣＲＬの更新日時と比較することで最新か否かが判断され、データＣＲＬｄａｔｅが最新と判断されたとき、ステップＳ１５２へ移行する。また、データＣＲＬｄａｔｅが最新でないときはステップＳ１６０へ移行する（ステップＳ１５０）。

【０１２２】データＣＲＬｄａｔｅが最新と判断されたとき、暗号処理部３２８は、暗号処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８をメモリカード１１０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ１５２）。

【０１２３】そして、携帯電話機１００のコントローラ１１０６は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１５４）、バスＢＳ５を介してメモリカード１１０に入力する。メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を端子１４２６およびインタフェース１４２４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を受理する（ステップＳ１５８）。その後、ステップＳ１７２へ移行する。

【０１２４】一方、配信サーバ１０において、ＣＲＬｄａｔｅが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の証明書失効リストのデータＣＲＬｄａｔｅを取得し、差分データである差分ＣＲＬを生成する（ステップＳ１６０）。

【０１２５】暗号処理部３２８は、暗号処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する証明書失効リストの差分ＣＲＬとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１６２）。

【０１２６】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１２７】携帯電話機１００は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１６４）、バスＢＳ２を介してメモリカード１１０に入力する（ステップＳ１６６）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３の受信データを復号しバスＢＳ３に出力する（ステップＳ１６８）。

【０１２８】この段階で、バスＢＳ３には、Ｋｍｃ保持部５２２１に保持される秘密復号鍵Ｋｍｃ８で復号可能な暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝と、差分ＣＲＬとが出力される（ステップＳ１６８）。コントローラ１４２０の指示によって受理した差分ＣＲＬによってメモリ１４１５内のＣＲＬ領域１４１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ１７０）。

【０１２９】ステップＳ１５２，Ｓ１５４，Ｓ１５６，Ｓ１５８は、メモリカード１１０が保持する証明書失効リストＣＲＬｄａｔｅが最新の場合のメモリカード１１０へのライセンスの配信動作であり、ステップＳ１６０，Ｓ１６２，Ｓ１６４，Ｓ１６６，Ｓ１６８，Ｓ１７０は、メモリカード１１０が保持する証明書失効リストＣＲＬが最新でない場合のメモリカード１１０へのライセンスの配信動作である。このように、メモリカード１１０から送られてきた証明書失効リストＣＲＬｄａｔｅが最新か否かを、逐一、確認し、最新でないとき、最新の証明書失効リストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをメモリカード１１０に配信す

ることによって、配信したライセンスが、秘密復号鍵が漏洩したり、ＴＲＭが破られた不正なメモリカードやコンテンツ再生デバイスへ出力されることを防止できる。

【０１３０】ステップＳ１５８またはステップＳ１７０の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限ＡＣｍおよび再生制限ＡＣｐ）が受理される（ステップＳ１７２）。

【０１３１】図１１を参照して、コントローラ１４２０は、受理したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限ＡＣｍおよび再生制限ＡＣｐ）をメモリ１４１５のライセンス領域１４１５Ｂに記録する（ステップＳ１７４）。

【０１３２】携帯電話機１００のコントローラ１１０６は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ１７８）。

【０１３３】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１８０）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１８２）。

【０１３４】携帯電話機１００は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１８４）。そして、コントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受取り、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１５１５Ｃに記録する（ステップＳ１９０）。そして、携帯電話機１００のコントローラ１１０６は、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ１９２）。

【０１３５】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ１９４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１９６）、全体の処理が終了する（ステップＳ１９８）。

【０１３６】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上で、クラス証明書Ｃｍ７が証明書失効リスト、すなわち、公開暗号鍵ＫＰｍ７による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１３７】［再生］次に、図１２および図１３を参照してメモリカード１１０に記録されたコンテンツデータのポータブルステレオ１２０（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。図１２を参照して、再生動作の開始とともに、ポータブルステレオ１２０のユーザから操作パネル２０１０を介して再生指示がポータブルステレオ１２０にインプットされる（ステップＳ１０００）。そうすると、コントローラ２０２０は、バスＢＳ４を介して認証データ保持部１５００から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを読出し、送受信部２００２を介して携帯電話機１００へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力する（ステップＳ１００２）。

【０１３８】そうすると、携帯電話機１００においてコントローラ１１０６は、アンテナ１１０３および送受信部１１０４を介して認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受信し、メモリカードインタフェース１２００を介して認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａをメモリカード１１０へ出力する。そして、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理する（ステップＳ１００４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ１００６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ１００８）。復号できなかった場合、ステップＳ１０４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｐ１がメモリ１４１５から読出した証明書失効リストデータＣＲＬに含まれるか否かを判断する（ステップＳ１０１０）。この場合、証明書Ｃｐ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｐ１のＩＤが証明書失効リストデータの中に存在するか否かを判別する。証明書Ｃｐ１が証明書失効リストデータに含まれると判断されると、ステップＳ１０４８へ移行し、再生動作は終了する。

【０１３９】ステップＳ１０１０において、証明書Ｃｐ

１が証明書失効リストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ１０１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ１０１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ１０１６）。携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得し、その取得した暗号化データ｛Ｋｓ２｝Ｋｐ１を送受信部１１０４を介してポータブルステレオ１２０へ送信する。そうすると、ポータブルステレオ１２０のコントローラ２０２０は、アンテナ２０００および送受信部２００２を介して暗号化データ｛Ｋｓ２｝Ｋｐ１を受信し、復号処理部１５０４へ暗号化データ｛Ｋｓ２｝Ｋｐ１を与える。そして、Ｋｐ保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０１４０】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ１０１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ１０２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ２０２０は、バスＢＳ４および送受信部２００２を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を携帯電話機１００へ送信する（ステップＳ１０２２）。

【０１４１】そうすると、携帯電話機１００のコントローラ１１０６は、送受信部１１０４を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を受信し、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を受信し、復号処理部１４１２へ与える（ステップＳ１０２４）。

【０１４２】図１３を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、ポータブルステレオ１２０のコンテンツ再生デバイス１５５０で発生されたセッションキーＫｓ３を受理する（ステップＳ１０２６）。セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、アクセス制限ＡＣｍを確認する（ステップＳ１０２８）。ステップＳ１０２８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限ＡＣｍを確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限に制限がある場合にはアクセス制限ＡＣｍのデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ１０３０）。一方、アクセス制限ＡＣｍによって再生回数が制限されていない場合においては、ステップＳ１０３０はスキップされ、アクセス制限ＡＣｍは更新されることなく処理が次のステップ（ステップＳ１０３２）に進行される。

【０１４３】ステップＳ１０２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制限ＡＣｐがバスＢＳ４上に出力される（ステップＳ１０３２）。

【０１４４】得られたライセンス鍵Ｋｃと再生制限ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生制限ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ１０３４）。

【０１４５】バスＢＳ３に出力された暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３は、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して携帯電話機１００に送出される。

【０１４６】携帯電話機１００のコントローラ１１０６は、暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を受取り、送受信部１１０４を介して暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をポータブルステレオ１２０へ送信する。そして、ポータブルステレオ１２０のコントローラ２０２０は、送受信部２００２を介して暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を受信し、その受信した暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０に与える。復号処理部１５１０は、暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をセッションキーＫｓ３によって復号し、ライセンス鍵Ｋｃおよび再生制限ＡＣｐを受理する（ステップＳ１０３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制限ＡＣｐをバスＢＳ４に出力する。

【０１４７】コントローラ２０２０は、バスＢＳ４を介して、再生制限ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ１０４０）。

【０１４８】ステップＳ１０４０においては、再生制限

ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０１４９】ステップＳ１０４０において再生可能と判断された場合、コントローラ２０２０は、送受信部２００２、携帯電話機１００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ１０４２）。

【０１５０】携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、送受信部１１０４を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをポータブルステレオ１２０へ送信する。ポータブルステレオ１２０のコントローラ２０２０は、送受信部２００２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受信し、バスＢＳ４を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０１５１】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する（ステップＳ１０４４）。

【０１５２】そして、復号されたコンテンツデータＤｃは音楽デコーダ１５１８へ出力され、音楽デコーダ１５１８は、コンテンツデータを再生し、再生したアナログ信号である音楽信号をＬチャネルスピーカ用の信号とＲチャネルスピーカ用の信号とに分離してＬＰＦ２０１６，２０１８へ出力する。そして、音楽信号はＬＰＦ２０１６，２０１８でノイズを除去され、増幅器２０２４，２０２６でゲイン制御部２０２２によって制御された増幅率に増幅され、スピーカ２０２８，２０３０から外部へ出力されて再生される（ステップＳ１０４６）。これによって再生動作が終了する。

【０１５３】上記においては、携帯電話機１００に装着されたメモリカード１１０に記録された暗号化コンテンツデータをポータブルステレオによって再生する場合について説明したが、ポータブルステレオ１２０にメモリカード１１０が装着された場合も、上述したフローチャートに従って暗号化コンテンツデータが再生される。

【０１５４】また、上述したように携帯電話機１００は、コンテンツ再生デバイス１５５０を内蔵するので、携帯電話機１００はメモリカード１１０に記録された暗号化コンテンツデータを上述したフローチャートに従って再生することが可能である。

【０１５５】本発明によるポータブルステレオは、図７に示すものに限らず、図１４に示すポータブルステレオ１２０Ａであっても良い。ポータブルステレオ１２０Ａは、本体１２１と、スピーカ２０２８，２０３２とから成り、携帯電話機１００Ａの充電台が設けられた携帯電話機充電台兼用型のポータブルステレオである。

【０１５６】図１５は、ポータブルステレオ１２０Ａのブロック図を示したものである。ポータブルステレオ１２０Ａは、図７に示すポータブルステレオ１２０に充電部２５００を追加したものであり、それ以外はポータブルステレオ１２０と同じである。充電部２５００は、電源２５０１と、電圧制御部２５０２と、誘導コイル２５０３とから成る。電圧制御部２５０２は電源２５０１から供給される電力に基づいて誘導コイル２５０３によって発生される電圧を制御する。誘導コイル２５０３は、電圧制御部２５０２によって制御された電圧を伝える、誘導磁界を発生させ、携帯電話機１００Ａを充電する。

【０１５７】図１６は、ポータブルステレオ１２０Ａに設置される携帯電話機１００Ａの構成を示すブロック図である。携帯電話機１００Ａは、図５に示す携帯電話機１００に充電部１１３０を追加したものであり、その他は携帯電話機１００と同じである。充電部１１３０は、誘導コイル１１３２と、電流制御部１１３４と、電池１１３６とから成る。誘導コイル１１３２は、ポータブルステレオ１２０の誘導コイル２５０３によって発生した誘導磁界に反応して、誘導電流を発生する。この時の電圧は、ポータブルステレオ１２０の電圧制御部２５０２によって制御される。誘導コイル１１３２は、電流制御部１１３４に誘導電流を供給し、電流制御部１１３４は、電池へ供給する電流を制御し、電池へ充電用電流を提供する。そして、電池１１３４は、電流制御部１１３４からの電流によって充電される。

【０１５８】図１６に示す携帯電話機１００Ａは、図８～図１１に示すフローチャートに従って配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信してメモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータおよびライセンスを記録する。そして、図１５に示すポータブルステレオ１２０Ａは、図１２，１３に示すフローチャートに従って携帯電話機１００Ａから暗号化コンテンツデータおよびライセンスを受信して再生する。

【０１５９】このように、携帯電話機と一体型になったポータブルステレオにおいては、携帯電話機を設置したままで、暗号化コンテンツデータおよびライセンスを配信サーバから受信できるとともに、メモリカードに記録された暗号化コンテンツデータをスムーズに再生できる。

【０１６０】本発明におけるポータブルステレオは、図１７に示すポータブルステレオ１２０Ｂであっても良い。ポータブルステレオ１２０Ｂは、ハンドフリーの機能付きポータブルステレオであり、図７に示すポータブルステレオ１２０に音声入力部１２４を追加したものである。そして、ポータブルステレオ１２０Ｂと通信する携帯電話機は、ポータブルステレオが音声入力部１２４

に対応した構成を有する携帯電話機１００Ｂである。その他は、図７に示すポータブルステレオ１２０と同じである。

【０１６１】図１８は、ポータブルステレオ１２０Ｂのブロック図を示したものである。ポータブルステレオ１２０Ｂは、図７に示すポータブルステレオ１２０に音声入力部１２４と、音声コーディック２０３４と、ＤＡ変換器２０１４と、混合器２０３６とを追加したものであり、それ以外は図７に示すポータブルステレオ１２０と同じである。

【０１６２】音声入力部１２４は、マイク１２４１と、増幅器１２４２と、バンドパスフィルタ（ＢＰＦ）１２４３と、ＡＤ変換機１２４４とから成る。マイク１２４１から入力された音声は増幅器１２４２で増幅され、ＢＰＦ１２４３でノイズを除去される。そして、音声は、マイク１２４１から入力されて、電気信号である音声信号としてＡＤ変換機１２４４に入力され、アナログ信号からデジタル信号に変換されて音声コーディック２０３４に入力される。

【０１６３】そうすると、音声コーディック２０３４は、送話信号を所定の方式に符号化した送話データとして送受信部２００２へ出力する。そして、送受信部２００２は、入力した送話データを携帯電話器１００Ｂへ送信する。また、携帯電話機から送信され、かつ、符号化された受話音声データは音声コーディック２０３４に入力され、受話音声データとして復号され、ＤＡ変換器２０１４にてデジタル信号からアナログ信号へ変換され、音声信号として混合器２０３６へ供給される。混合器２０３６は音声信号と、音楽デコーダ１５１８の出力である音楽信号を、コントローラ２０２０の指示に従って、選択的あるいは混合して２つのＬＰＦ２０１６，２０１８へ出力するものである。

【０１６４】つまり、ポータブルステレオ１２０Ｂは、音声入力部１２４からユーザの音声を入力し、その音声を携帯電話機１００Ｂを介して外部と通話する機能を有するポータブルステレオであり、自動車に搭載されるカーステレオとしてハンズフリー通話機能を付加したものとして用いることができる。同様に、ポータブルステレオ１２０および１２０Ａについてもカーステレオとして用いることが可能である。

【０１６５】図１９は、図１８に示すポータブルステレオ１２０Ｂからの音声信号を受け、その受けた音声信号を外部へ送信する機能を有する携帯電話機である。したがって、携帯電話機１００Ｂは、外部へ音声を送受信するアンテナ１１０１および送受信部１１０２と、ポータブルステレオ１２０Ｂとの信号を送受信するアンテナ１１０３および送受信部１１０４とを有する。

【０１６６】図１９に示す携帯電話機１００Ｂは、図８～図１１に示すフローチャートに従って配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信してメモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータおよびライセンスを記録する。そして、図１８に示すポータブルステレオ１２０Ｂは、図１２，１３に示すフローチャートに従って携帯電話機１００Ｂから暗号化コンテンツデータおよびライセンスを受信して再生するとともに携帯電話機１００Ｂを介して外部と通話する。

【０１６７】本発明においては、ポータブルステレオ１２０および１２０Ａは、配信を受ける機能を備える携帯電話機１００および１００Ａに変えて、再生専用機を用いることも可能である。その場合、再生専用機は、携帯電話機１００および１００Ａを備える、携帯電話網を介した通話および配信の受信に用いる通信機能を省いた構成となる。

【０１６８】携帯電話器１００Ａに対応する再生専用機１００Ｃは、図２０に示すようにアンテナ１１０３と、送受信部１１０４と、充電部１１３０と、コンテンツ再生デバイス１５５０と、コントローラ１１０６と、表示パネル１１０８と、操作パネル１１１０と、メモリカードインタフェース１２００とを備える。

【０１６９】同様に、図示しないが、携帯電話機１００に対応する再生専用機は、図２０の再生専用機１００Ｃにおける充電部１１３０を省いた構成となる。

【０１７０】なお、上述したポータブルステレオ１２０，１２０Ａ、および１２０Ｂは、携帯電話機または再生専用機からの暗号化コンテンツデータを再生する他、メモリカードインタフェース２０３０にメモリカード１１０を装着することで、直接メモリカードからライセンス鍵と暗号化コンテンツデータを取得して、音楽を再生することが可能である。この場合、送受信部２００２を介して行なうデータの授受を、メモリカードインタフェース２０３０を介して、直接メモリカード１１０との間で行うようにすればよく、再生動作は図１２および図１３のフローチャートに従う。

【０１７１】また、ポータブルステレオ１２０，１２０Ａおよび１２０ＢはＣＤ、カセットテープ、ＭＤ等の再生機能を備えた構成として、ＣＤ、カセットテープ、ＭＤ等に記録された平文の音楽データも再生するものとしてもよい。

【０１７２】さらに、ポータブルステレオ１２０，１２０Ａおよび１２０Ｂはメモリカードインタフェース２０３０を備えない構成としても良い。

【０１７３】また、上記においては、メモリカード１１０は、携帯電話機１００を用いて配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信するとして説明したが、本発明においては、メモリカード１１０は音楽データが記録された音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得しても良い。一般には、メモリカード１１０は、どんな方法によって暗号化コンテンツデータおよびライセンスを

31

取得しても良い。したがって、本発明は、暗号化コンテンツデータおよびライセンスを記録したメモリカードから通信によって暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータを再生するポータブルステレオに適用される。

【０１７４】本発明の実施の形態によれば、ポータブルステレオは、暗号化コンテンツデータおよびライセンスを記録したメモリカードが装着された携帯電話機から暗号化コンテンツデータおよびライセンスを受信して再生するので、通信機能を有しないカーステレオまたはコンポーネントステレオであっても、暗号化コンテンツデータを再生できる。

【０１７５】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　本発明の実施の形態におけるデータ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図５】　図１に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおけるポータブルステレオの構成を示す概略ブロック図である。

【図８】　図１に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第１のフローチャートである。

【図９】　図１に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第２のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第３のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第４のフローチャートである。

【図１２】　図１に示すデータ配信システムにおける携帯電話機における再生動作を説明するための第１のフローチャートである。

【図１３】　図１に示すデータ配信システムにおける携帯電話機における再生動作を説明するための第２のフローチャートである。

32

【図１４】　図１に示すデータ配信システムにおけるポータブルステレオの他の構成図である。

【図１５】　図１に示すデータ配信システムにおけるポータブルステレオの他の概略ブロック図である。

【図１６】　図１に示すデータ配信システムにおける携帯電話機の他の概略ブロック図である。

【図１７】　図１に示すデータ配信システムにおけるポータブルステレオのさらに他の構成図である。

【図１８】　図１に示すデータ配信システムにおけるポータブルステレオのまたさらに他の概略ブロック図である。

【図１９】　図１に示すデータ配信システムにおける携帯電話機のさらに他の概略ブロック図である。

【図２０】　再生専用機の構成を示す概略ブロック図である。

【符号の説明】

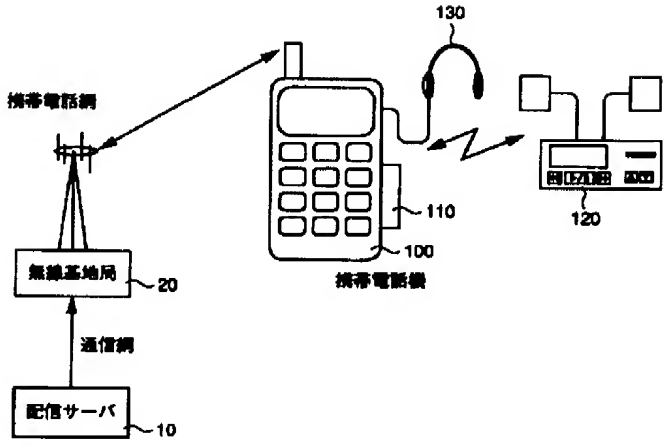
１０　配信サーバ、２０　無線基地局、１００，１００Ａ，１００Ｂ　携帯電話機、１１０　メモリカード、１２０，１２０Ａ，１２０Ｂ　ポータブルステレオ、１００Ｃ　再生専用機、１２１　本体、１２４　音声入力部、１３０　ヘッドホーン、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、３５０　通信装置、１１０６，１４２０，２０２０　コントローラ、１１０１，１１０３，２０００　アンテナ、１１０２，１１０４，２００２　送受信部、１１１４，１１２０，１１２４，１４２６　端子、１１０８，２０１０　操作パネル、１１１０，２００８　表示パネル、１１１２　音声処理部、１１１４，１２４１マイク、１１１６，２０２８，２０３２　スピーカ、１１１８，２０３６　混合器、１１２２　外部インタフェース、１１２６，１１２８，２０３４　音声コーディック、１１３４　電流制御部、１１３６　電池、１２００，２０３０　メモリカードインタフェース、１２４３　ＢＰＦ、１２４４　ＡＤ変換器、１４００，１５００　認証データ保持部、１４０２　Ｋｍｃ保持部、１４１４　ＫＰａ保持部、１４１５　メモリ、１４１５Ａ　ＣＲＬ領域、１４１５Ｂ　ライセンス領域、１４１５Ｃ　データ領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ保持部、１５１８　音楽デコーダ、２０１２，２０１４　ＤＡ変換器、１５５０　コンテンツ再生デバイス、２０１６，２０１８　ＬＰＦ、２

33

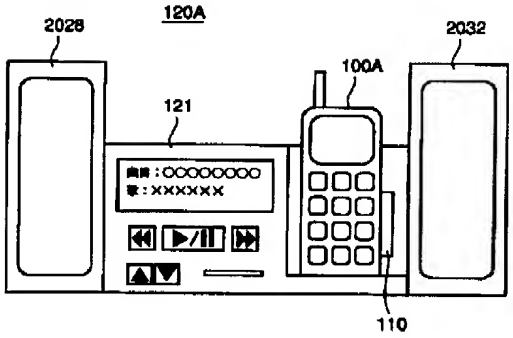
０２２ゲイン制御部、１２４２，２０２４，２０２６　増幅器、１１３０，２５００充電部、２５０１　電源、２５０２　電圧制御部、１１３２，２５０３　誘導コイル。

34

【図１】



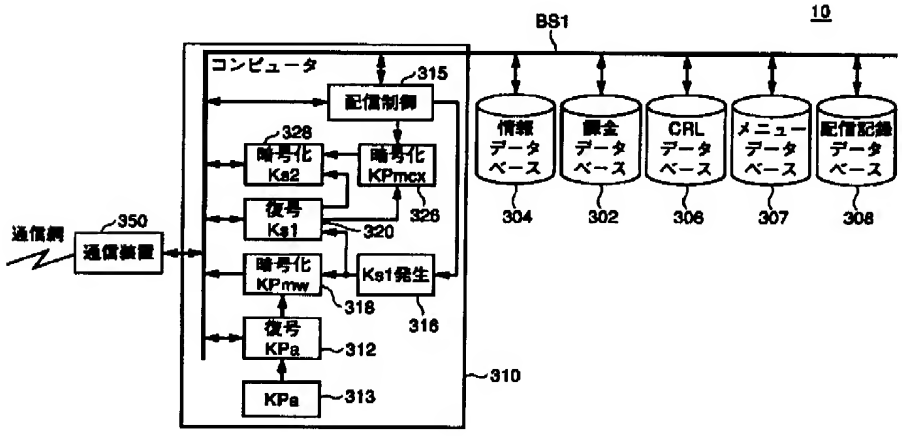
【図１４】



【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ (Dc)Kcとして配信され、メモリカードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	ライセンス固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止疑似データのリスト CRLの更新日(CRLdate)を含む

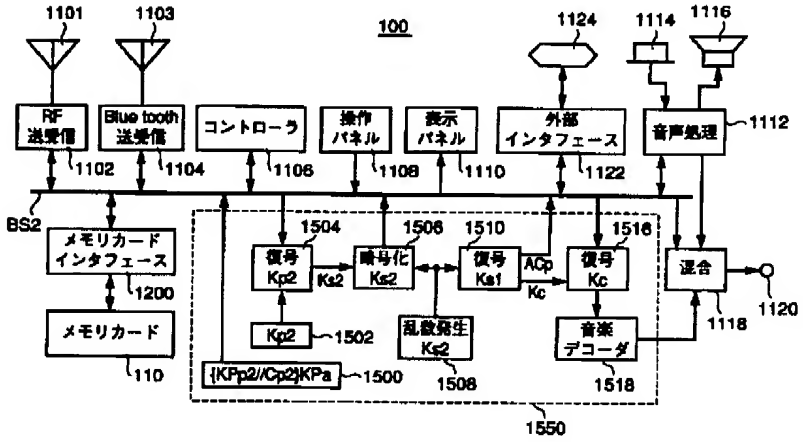
【図４】



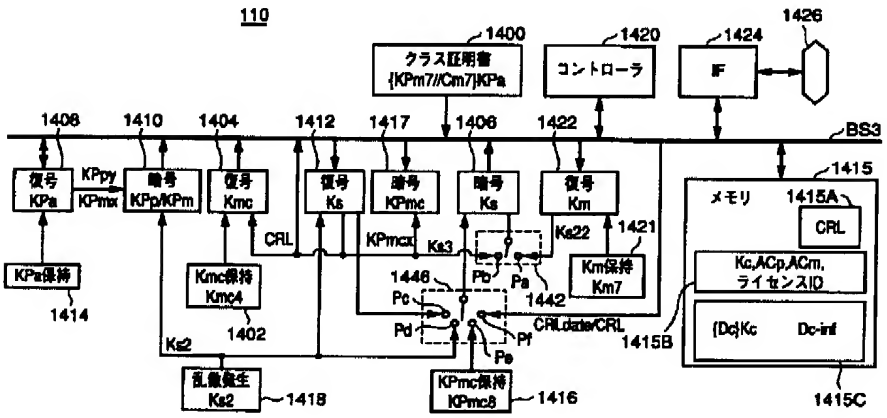
【図３】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証された認証データを復号する鍵 メモリカードおよびコンテンツ管理モジュールと同一
	Ks1	共通鍵	セッション固有	メモリカードへのライセンスの配信毎に発生
メモリカード	KPa	公開認証鍵	システム共通	認証局にて認証された認証データを復号する鍵 配信サーバと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受毎に発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 {KPmw//Cmw}KPaの形式で出荷時に記録。 ※メモリカードのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッション毎に発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy//Cpy}KPaの形式で出荷時に記録。 ※コンテンツ再生デバイスのクラスyごとに異なる。

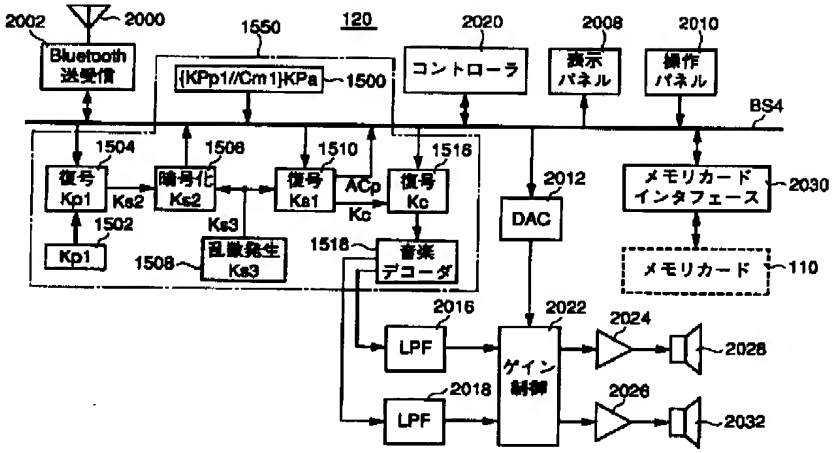
【図５】



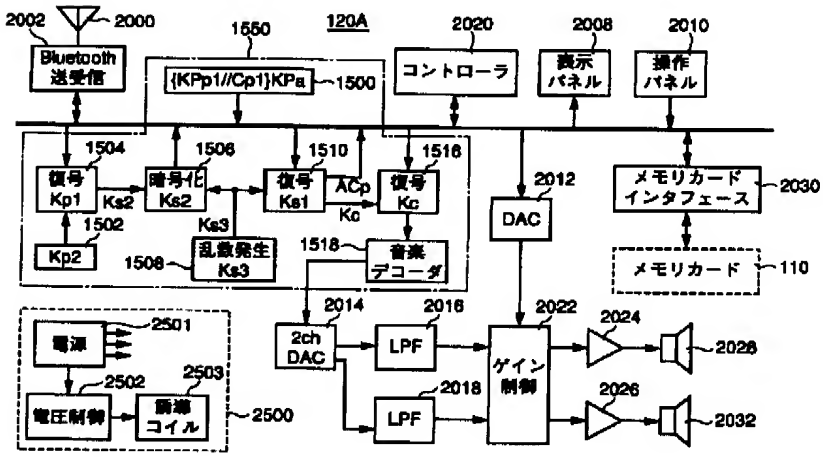
【図６】



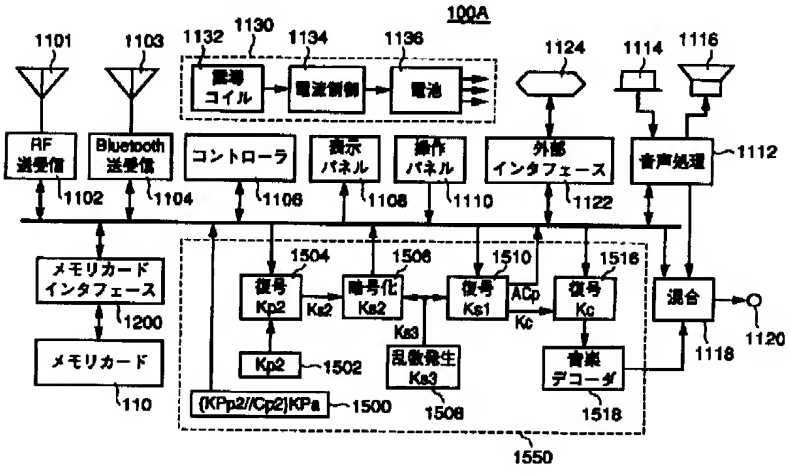
【図７】


2002
2000
Bluetooth 送受信
1550
120
{KPp1//Cm1}KPa
1500
コントローラ
2020
表示パネル
2008
操作パネル
2010
BS4
1504
復号 Kp1
Ks2
1506
暗号化 Ks2
1510
復号 Ks1
ACp
Kc
1518
復号 Kc
Ks3
1502
Kp1
1508
乱数発生 Ks3
1518
音楽デコーダ
2012
DAC
メモリカードインタフェース
2030
メモリカード
110
2016
LPF
2022
ゲイン制御
2024
2028
2018
LPF
2026
2032

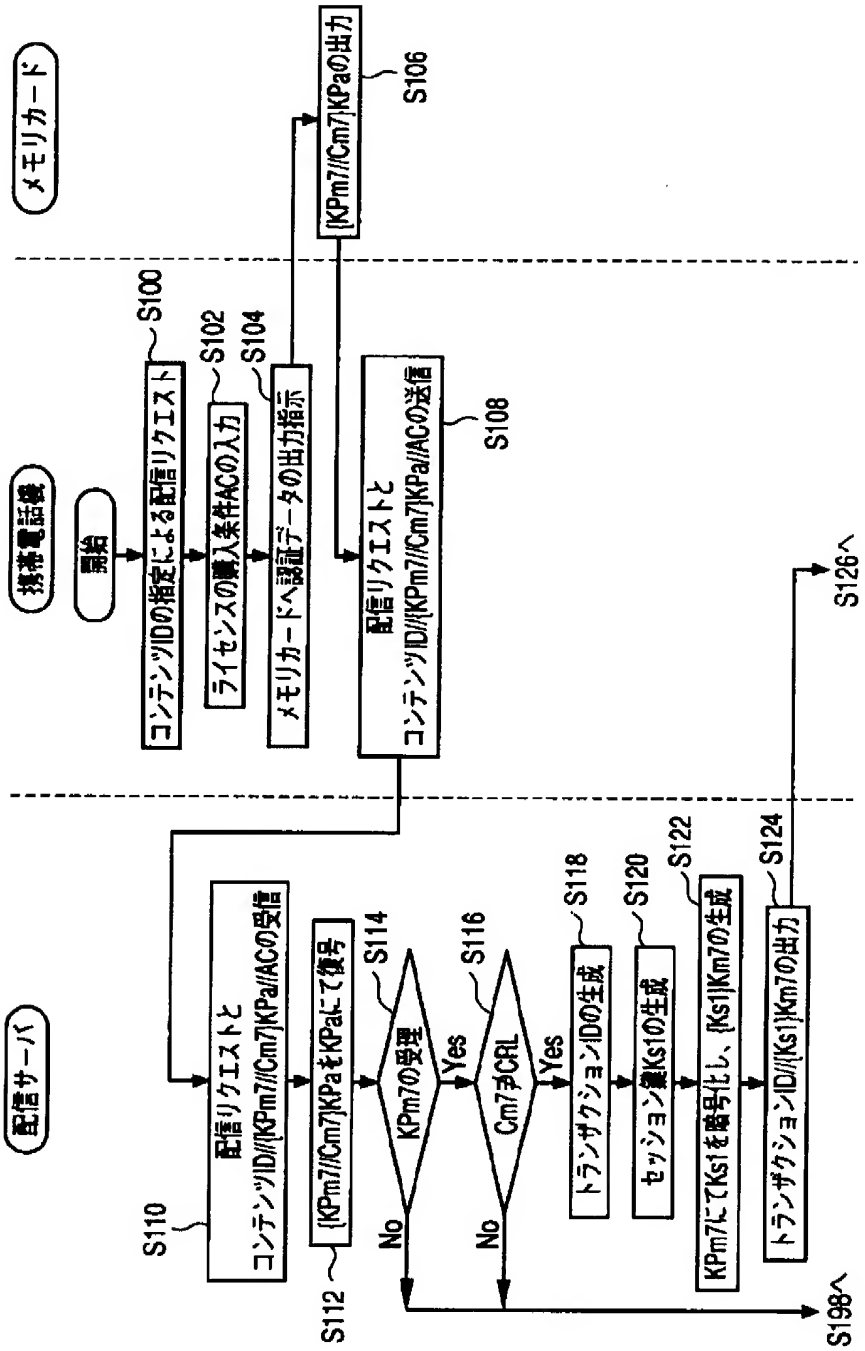
【図１５】


2002
2000
Bluetooth 送受信
1550
120A
{KPp1//Cp1}KPa
1500
コントローラ
2020
表示パネル
2008
操作パネル
2010
1504
復号 Kp1
Ks2
1506
暗号化 Ks2
1510
復号 Ks1
ACp
Kc
1516
復号 Kc
Ks3
1502
Kp2
1508
乱数発生 Ks3
1518
音楽デコーダ
2012
DAC
メモリカードインタフェース
2030
メモリカード
110
2501
電源
2502
電圧制御
2503
振源コイル
2500
2014
2ch DAC
2016
LPF
2022
ゲイン制御
2024
2028
2018
LPF
2026
2032

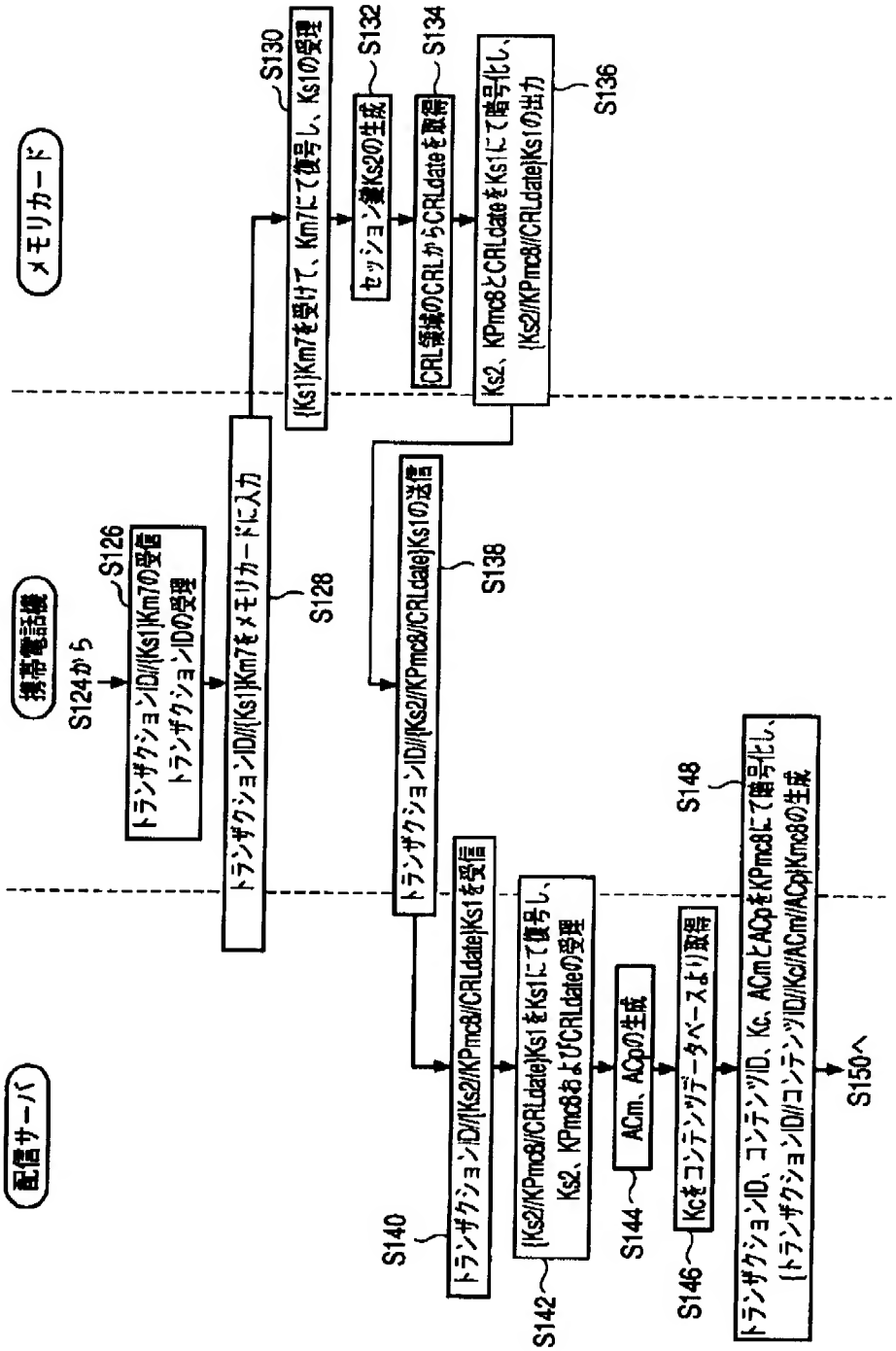
【図１６】


100A
1101
1103
1132
1130
1134
1136
1124
1114
1116
振源コイル
電源制御
電池
RF 送受信
Bluetooth 送受信
コントローラ
表示パネル
操作パネル
外部インタフェース
音声処理
1112
1102
1104
1106
1108
1110
1122
メモリカードインタフェース
1200
メモリカード
110
1504
復号 Kp2
Ks2
1506
暗号化 Ks2
1510
復号 Ks1
ACp
Kc
1516
復号 Kc
Ks3
Kp2
1502
乱数発生 Ks3
音楽デコーダ
混合
1118
1120
{KPp2//Cp2}KPa
1500
1508
1518
1550

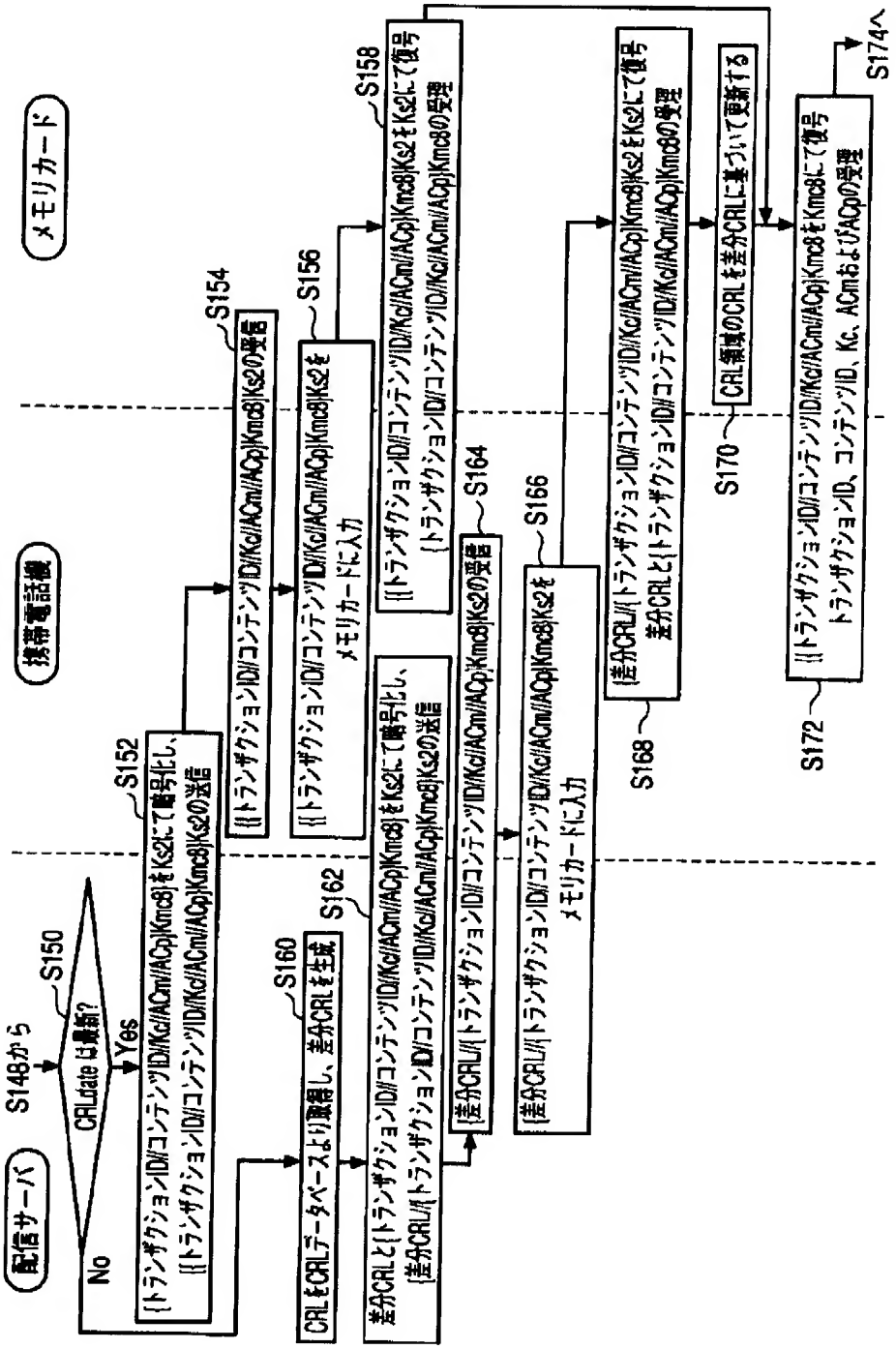
【図８】


メモリカード
携帯電話機
配信サーバ
開始
S100
コンテンツIDの指定による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
メモリカードへ認証データの出力指示
S106
{KPm7}{Cm7}KPaの出力
S108
配信リクエストと
コンテンツID//{KPm7}{Cm7}KPa//ACの送信
S110
配信リクエストと
コンテンツID//{KPm7}{Cm7}KPa//ACの受信
S112
{KPm7}{Cm7}KPaをKPaにて復号
S114
KPm7の受理
No
Yes
S116
Cm7≠CRL
No
Yes
S118
トランザクションIDの生成
S120
セッション鍵Ks1の生成
S122
KPm7にてKs1を暗号化し、{Ks1}Km7の生成
S124
トランザクションID//{Ks1}Km7の出力
S126へ
S198へ

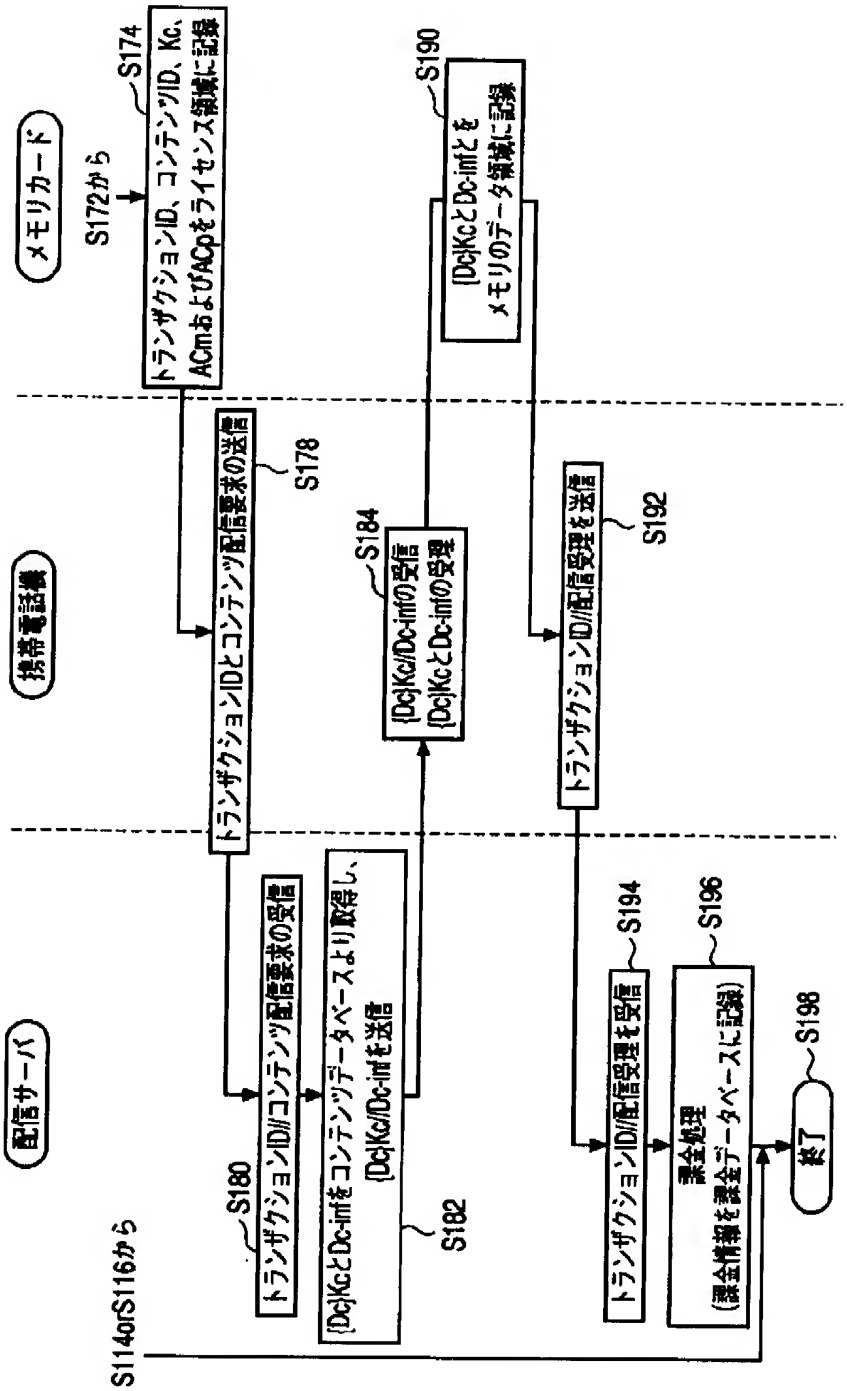
【図９】


メモリカード
携帯電話機
配信サーバ
S124から
トランザクションID//{Ks1}Km7の受信
トランザクションIDの受理
S126
トランザクションID//{Ks1}Km7をメモリカードに入力
S128
{Ks1}Km7を受けて、Km7にて復号し、Ks1の受理
S130
セッション鍵Ks2の生成
S132
CRL領域のCRLからCRLdateを取得
S134
Ks2、KPmc8とCRLdateをKs1にて暗号化し、
{Ks2//KPmc8//CRLdate}Ks1の出力
S136
トランザクションID//{Ks2//KPmc8//CRLdate}Ks1の送信
S138
トランザクションID//{Ks2//KPmc8//CRLdate}Ks1を受信
S140
{Ks2//KPmc8//CRLdate}Ks1をKs1にて復号し、
Ks2、KPmc8およびCRLdateの受理
S142
ACm、ACpの生成
S144
Kcをコンテンツデータベースより取得
S146
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc8にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の生成
S148
S150へ

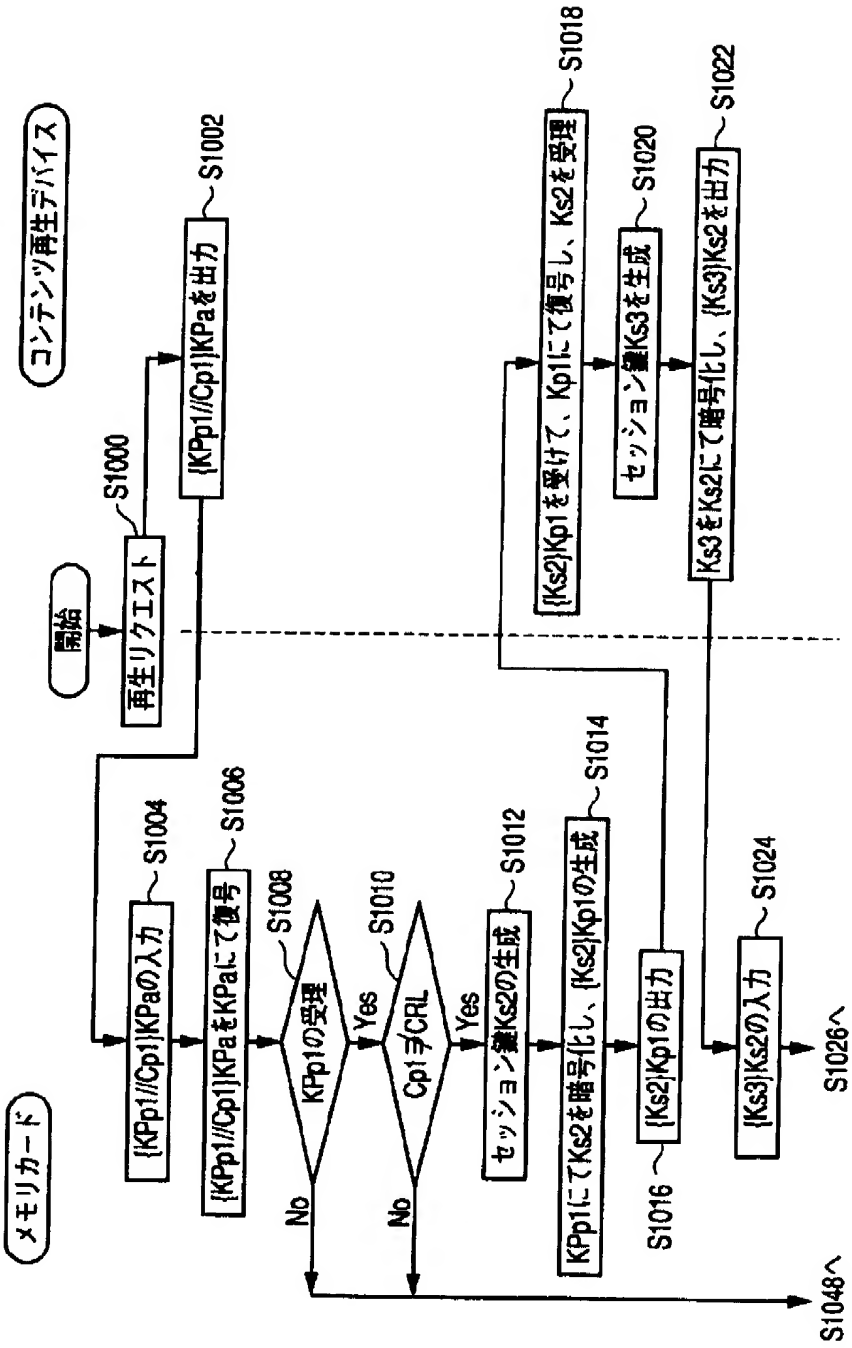
【図１０】


配信サーバ
携帯電話機
メモリカード
S148から
S150
CRLdate は最新?
No
Yes
S152
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2の送信
S154
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2の受信
S156
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2を
メモリカードに入力
S158
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8の受理
S160
CRLをCRLデータベースより取得し、差分CRLを生成
S162
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)をKs2にて暗号化し、
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2の送信
S164
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2の受信
S166
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2を
メモリカードに入力
S168
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)Ks2をKs2にて復号
差分CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8の受理
S170
CRL領域のCRLを差分CRLに基づいて更新する
S172
{{トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8)をKmc8にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S174へ

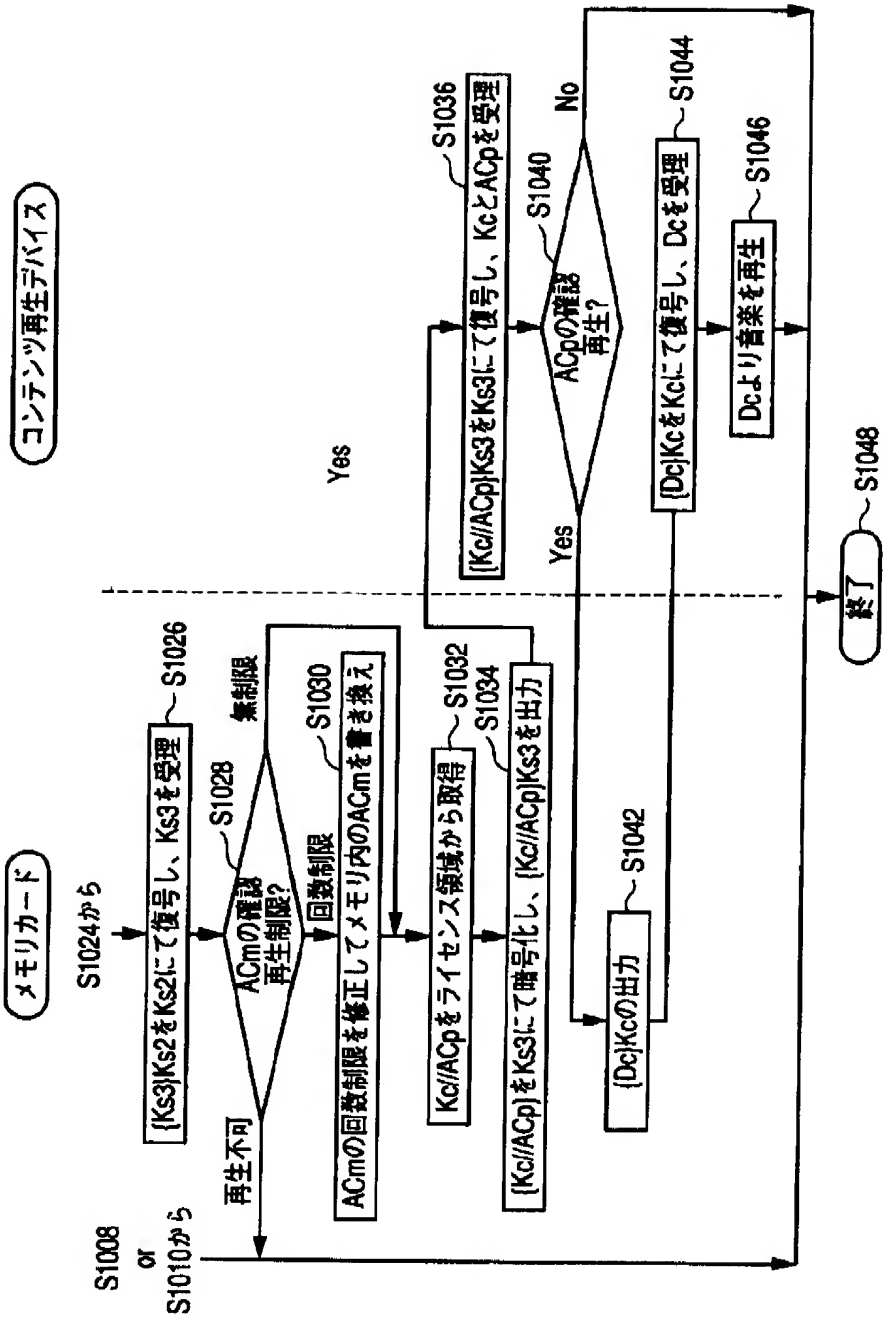
【図１１】


メモリカード
携帯電話機
配信サーバ
S172から
S174
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域に記録
S178
トランザクションIDとコンテンツ配信要求の送信
S180
トランザクションID//コンテンツ配信要求の受信
S182
{Dc}Kc/Dc-infをコンテンツデータベースより取得し、{Dc}Kc/Dc-infを送信
S184
{Dc}Kc/Dc-infの受信
{Dc}KcとDc-infの受理
S190
{Dc}KcとDc-infとをメモリのデータ領域に記録
S192
トランザクションID//配信受理を送信
S194
トランザクションID//配信受理を受信
S196
課金処理
(課金情報を課金データベースに記録)
S198
終了
S114orS116から

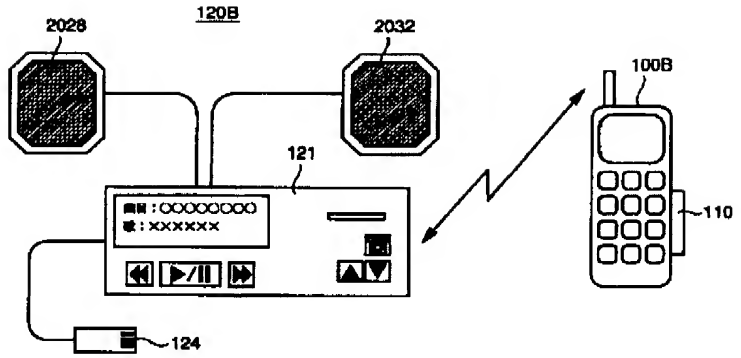
【図１２】


コンテンツ再生デバイス
メモリカード
開始
再生リクエスト
S1000
{KPp1//Cp1}KPaを出力
S1002
{KPp1//Cp1}KPaの入力
S1004
{KPp1//Cp1}KPaをKPaにて復号
S1006
KPp1の受理
S1008
No
Yes
Cp1ヲCRL
S1010
No
Yes
セッション鍵Ks2の生成
S1012
KPp1にてKs2を暗号化し、{Ks2}Kp1の生成
S1014
{Ks2}Kp1の出力
S1016
{Ks2}Kp1を受けて、Kp1にて復号し、Ks2を受理
S1018
セッション鍵Ks3を生成
S1020
Ks3をKs2にて暗号化し、{Ks3}Ks2を出力
S1022
{Ks3}Ks2の入力
S1024
S1026へ
S1048へ

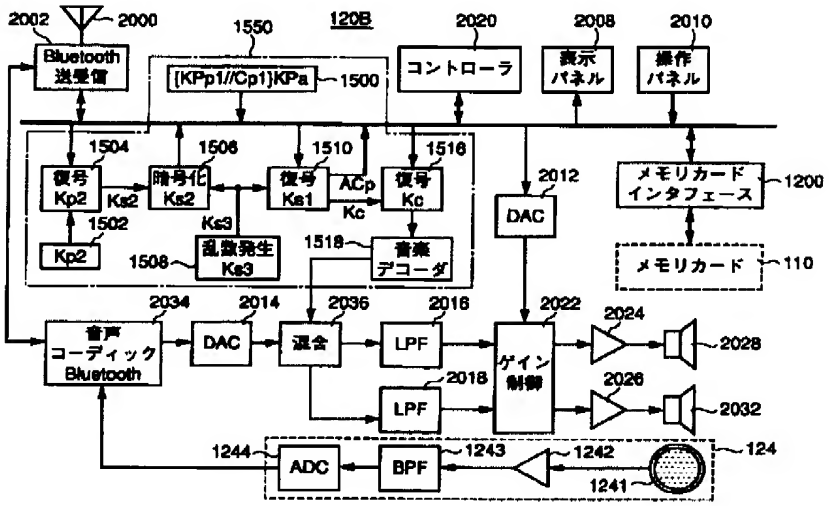
【図１３】


メモリカード
コンテンツ再生デバイス
S1024から
S1026
{Ks3}Ks2をKs2にて復号し、Ks3を受理
S1028
ACmの確認
再生制限?
無制限
回数制限
再生不可
S1030
ACmの回数制限を修正してメモリ内のACmを書き換え
S1008
or
S1010から
S1032
Kc//ACpをライセンス領域から取得
S1034
{Kc//ACp}Ks3にて暗号化し、{Kc//ACp}Ks3を出力
S1036
{Kc//ACp}Ks3をKs3にて復号し、KcとACpを受理
S1040
ACpの確認
再生?
Yes
No
Yes
S1042
{Dc}Kcの出力
S1044
{Dc}Kcを Kcにて復号し、Dcを受理
S1046
Dcより音楽を再生
S1048
終了

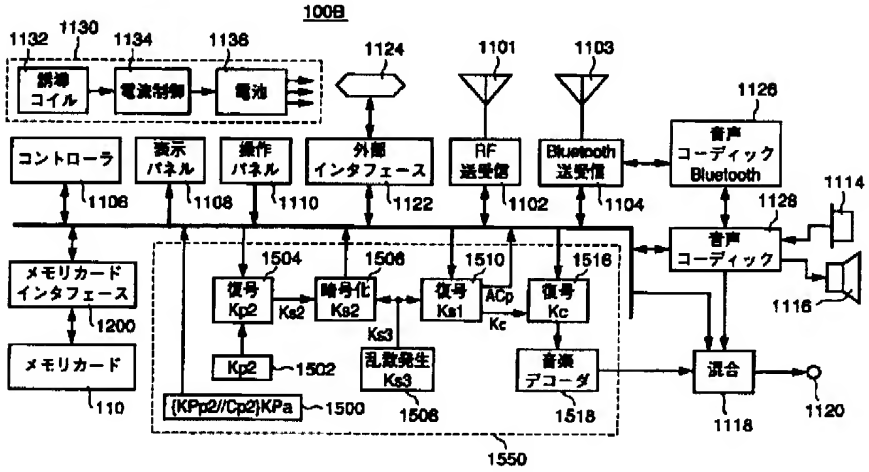
【図１７】


120B
2028
2032
100B
121
110
124

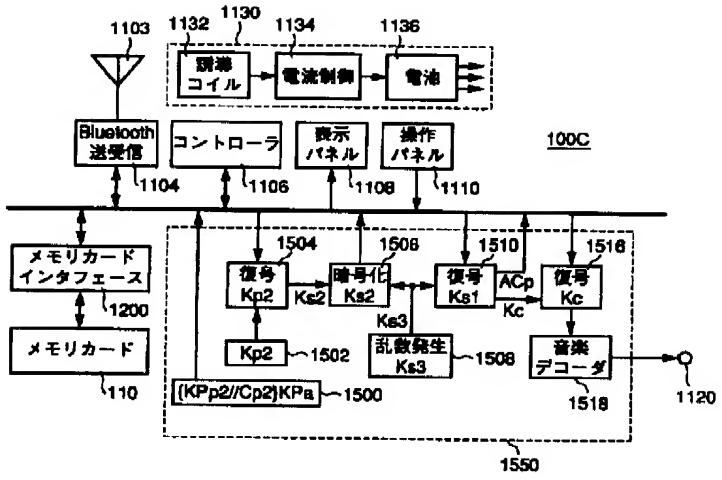
【図１８】


2002
2000
1550
120B
2020
2008
2010
Bluetooth 送受信
[KPp1//Cp1]KPa
1500
コントローラ
表示パネル
操作パネル
1504
1506
1510
1516
復号 Kp2
Ks2
暗号化 Ks2
復号 Ks1
ACp
Kc
復号 Kc
2012
DAC
メモリカードインタフェース
1200
1502
Kp2
Ks3
1508
乱数発生 Ks3
1518
音楽デコーダ
メモリカード
110
2034
2014
2036
2016
2022
2024
音声コーディック Bluetooth
DAC
混合
LPF
ゲイン制御
2028
2018
2026
2032
1244
ADC
BPF
1243
1242
1241
124

【図１９】


100B
1132
1130
1134
1136
誘導コイル
電流制御
電池
1124
1101
1103
1126
コントローラ
表示パネル
操作パネル
外部インタフェース
RF 送受信
Bluetooth 送受信
音声コーディック Bluetooth
1106
1108
1110
1122
1102
1104
1128
1114
メモリカードインタフェース
1200
メモリカード
110
1504
1506
1510
1516
復号 Kp2
Ks2
暗号化 Ks2
復号 Ks1
ACp
Kc
復号 Kc
Ks3
Kp2
1502
乱数発生 Ks3
音楽デコーダ
音声コーディック
1116
混合
1120
1118
{KPp2//Cp2}KPa
1500
1508
1518
1550

【図２０】



フロントページの続き

(51) Int. Cl.[7]		識別記号	FI		テーマコード（参考）
H04L	9/32		H04N	7/16	Z
H04M	1/00		G10L	9/00	N
	11/00	302	H04L	9/00	601A
H04N	7/16				601E
					675B

Fターム（参考） 5B017 AA06 BA09 CA00
5C064 BA07 BB02 BC03 BC04 BC06
BC17 BC18 BC22 BC23 BC25
BD02 BD03 BD04 BD08 BD09
CA14 CA16 CB01 CC01 CC04
5J104 AA07 AA15 AA16 EA06 EA18
KA02 KA05 NA02 NA03 NA35
NA37 NA38 NA41 PA02 PA11
5K027 AA11 BB09 CC08 FF28 HH24
HH29 KK02
5K101 KK18 LL12 NN07 NN15 NN21
UU19